UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,296	09/10/2003	Catherine M. Keene	AGIL-00501	5469

7590 07/09/2004

David R. Stevens
Stevens Law Group
P.O. Box 1667
San Jose, CA 95109

EXAMINER	
PHAM, HUNG Q	
ART UNIT	PAPER NUMBER
2172	

DATE MAILED: 07/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/660,296	**Applicant(s)** KEENE ET AL.	
	Examiner HUNG Q PHAM	**Art Unit** 2172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/09/2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Priority

1. An application in which the benefits of an earlier application are desired must contain a specific reference to the prior application(s) in the first sentence of the specification or in an application data sheet (37 CFR 1.78(a)(2) and (a)(5)). The specific reference to any prior nonprovisional application must include the relationship (i.e., continuation, divisional, or continuation-in-part) between the applications except when the reference is to a prior application of a CPA assigned the same application number.

Drawings

2. The drawing of FIG. 8 is objected to because the top margin of FIG. 8 does not have a top margin of at least 2.5 cm. (1 inch).

Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled “Replacement Sheet” in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 9-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 9 and 10 recite the limitation ***wherein*** ***establishing an object***. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation ***wherein*** ***verifying the requestor’s user privilege access criteria***. There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites the limitation ***wherein*** ***transmitting a redacted object***. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-5 and 7-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher et al. [USP 6,085,191].

Regarding to claim 1, Fisher teaches a system and method for controlling access to managed objects in a computer network.

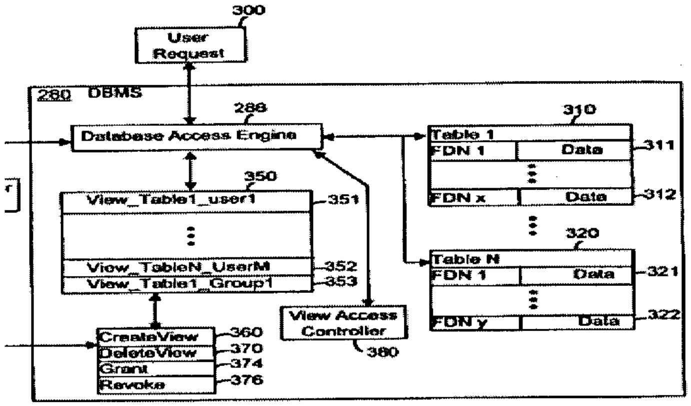
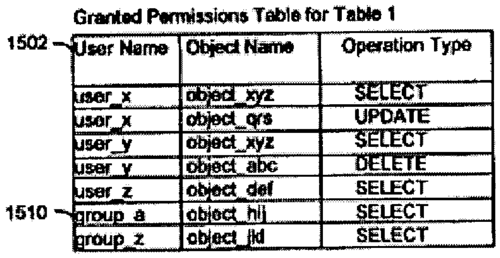


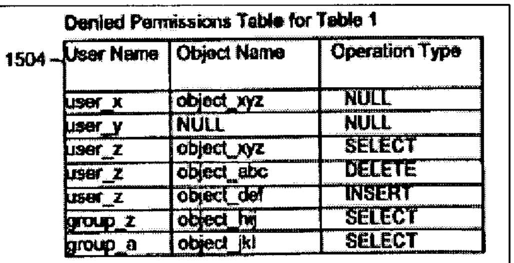
FIG. 10



Granted Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	SELECT
user_x	object_qrs	UPDATE
user_y	object_xyz	SELECT
user_y	object_abc	DELETE
user_z	object_def	SELECT
group_a	object_hij	SELECT
group_z	object_jkl	SELECT

FIG. 15A



Denied Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	NULL
user_y	NULL	NULL
user_z	object_xyz	SELECT
user_z	object_abc	DELETE
user_z	object_def	INSERT
group_z	object_hij	SELECT
group_a	object_jkl	SELECT

FIG. 15B

As shown in FIG. 10 is a conventional DBMS 280 for storing tables 310, 320 (Col. 18, Lines 39-42). As seen, table 310 with each row as shown above indicates ***an object and associated information***. Each row of table 310 has FDN or Fully Distinguished Name as the primary key to the data, and management information (Col. 19, Lines 1-29) as ***distinguishable group of data***. As shown in FIG. 15A is a permission table, each permission entry includes the FDN, and the operation types such as select, delete, insert or update operation (Col. 25, Lines 38-60). The rows of table 310 represented by FDN as ***groups of data having associated*** operation type as ***access criteria for accessing*** such as select, delete, insert or update operation. In short, the technique as discussed indicates the claimed ***a database for storing an object and associated information, the object comprising distinguishable groups of data, each group of data having associated access criteria for access to the groups of data***. Fisher further discloses ***a central processing unit (CPU) for controlling the access to the database; a memory for storing*** access control procedures as ***software code for controlling the operation of the CPU; and*** access control database contains access control rules to each access request as ***access application code stored in the memory and executable by the CPU*** (Col. 7, Lines 25-35). Fisher does not explicitly teach ***the application code being responsive to the access criteria associated with the groups of data contained within an object and to predetermined privileges for allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges***. However, Fisher teach that when checking whether access should be permitted for a particular operation, the access control procedure 404 checks both Grant and Deny tables as in FIG. 15A and B, which reflect the specified access rules, wherein the user name whose access rights are represented, and the operation type that the specified user is being granted or denied with respect to the specified object. For example, if the rule in the access control database specifies a “global grant” to user U1 for operation type Op1, an entry is made in the grant table, which is [U1, NULL, Op1] (Col. 25, Lines 51-Col. 26, Lines 52). As seen, “global grant” as ***an application code*** that allows access to a row of table 310 has FDN or Fully Distinguished Name as the primary key to the data, obviously, executed by the CPU, and in ***response to*** Op1 as ***the access criteria associated with the groups of data contained within an object***, and Op1 is also a user's ***predetermined privilege for allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges***. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher system by executing the access rule in response to access criteria in order to control access to managed objects in a computer network.

Regarding to claim 2, Fisher teaches all the claimed subject matters as discussed in claim 1, Fisher further discloses ***access includes the ability of a user to read the contents of the requested object*** (FIG. 15A).

Regarding to claim 3, Fisher teaches all the claimed subject matters as discussed in claim 2, Fisher further discloses ***access includes the ability to modify the contents of the requested object*** (FIG. 15A).

Regarding to claim 4, Fisher teaches all the claimed subject matters as discussed in claim 3, Fisher further discloses ***the ability to modify includes the ability to delete information contained in the requested object*** (FIG. 15A).

Regarding to claim 5, Fisher teaches all the claimed subject matters as discussed in claim 3, Fisher further discloses ***the ability to modify includes the ability to add data to the requested object*** (Col. 11, Lines 8-17).

Regarding to claim 7, Fisher teaches a system and method for controlling access to managed objects in a computer network.

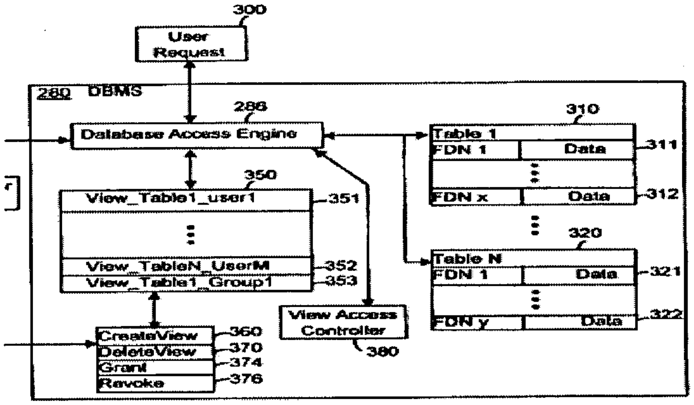
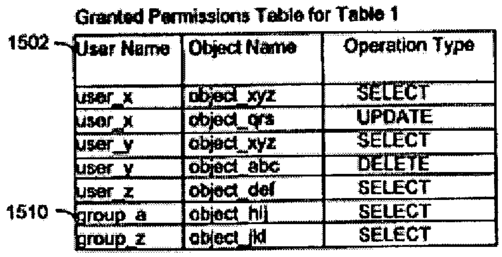


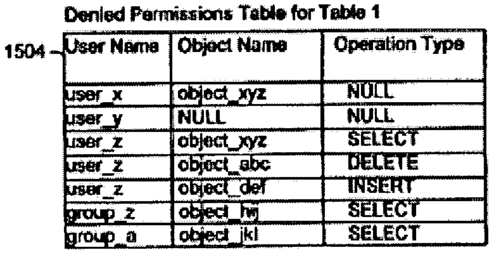
FIG. 10



Granted Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	SELECT
user_x	object_qrs	UPDATE
user_y	object_xyz	SELECT
user_y	object_abc	DELETE
user_z	object_def	SELECT
group_a	object_hij	SELECT
group_z	object_jkl	SELECT

FIG. 15A



Denied Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	NULL
user_y	NULL	NULL
user_z	object_xyz	SELECT
user_z	object_abc	DELETE
user_z	object_def	INSERT
group_z	object_hij	SELECT
group_a	object_jkl	SELECT

FIG. 15B

As shown in FIG. 10 is a conventional DBMS 280 for storing tables 310, 320 (Col. 18, Lines 39-42). As seen, table 310 with each row as shown above indicates ***an object and associated information***. Each row of table 310 has FDN or Fully Distinguished Name as the primary key to the data, and management information (Col. 19, Lines 1-

29) as ***distinguishable group of data***. As shown in FIG. 15A is a permission table, each permission entry includes the FDN, and the operation types such as select, delete, insert or update operation (Col. 25, Lines 38-60). The rows of table 310 represented by FDN as ***groups of data having associated*** operation type as ***access criteria for accessing*** such as select, delete, insert or update operation. In short, the technique as discussed indicates the claimed ***storing an object, the object comprising distinguishable groups of data, each group of data having associated access criteria for access to the groups of data***. Fisher further discloses access control procedures are executed by central processing unit (Col. 7, Lines 25-30), and both the tables above are checked by the access control procedure whether access should be permitted for a particular operation (Col. 25, Line 65-Col. 26, Line 2) as the step of ***controlling the access to the database using a central processing unit (CPU) according to access criteria***. The access control procedures as ***software code for controlling the operation of the CPU***, are ***stored in memory*** (Col. 7, Lines 25-35). Fisher does not explicitly teach the step of ***allowing controlled access to individual groups of data contained within the object by an individual user according to the user's privileges in response to the access criteria associated with the groups of data contained within an object and to predetermined privileges***. However, Fisher teach that when checking whether access should be permitted for a particular operation, the access control procedure 404 checks both Grant and Deny tables as in FIG. 15A and B, which reflect the specified access rules, wherein the user name whose access rights are represented, and the operation type that the specified user is being granted or denied with respect to the specified object. For example, if the rule in the access control

database specifies a "global grant" to user U1 for operation type Op1, an entry is made in the grant table, which is [U1, NULL, Op1] (Col. 25, Lines 51-Col. 26, Lines 52). As seen, ***access to individual groups of data contained within the object*** is ***controlled*** by the two tables, Grant and Deny, obviously, according to a user's particular operation as ***user's privilege***, and obviously, ***in response to*** Op1 as ***the access criteria associated with the groups of data contained within an object***, and Op1 is also a user's ***predetermined privilege***. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher system by allowing controlled access in response to access criteria in order to control access to managed objects in a computer network.

Regarding to claim 8, Fisher teaches all the claimed subject matters as discussed in claim 7, Fisher further discloses the step of ***receiving an object request by a requester; verifying the requestor's user privilege access criteria; and transmitting information according to the requestor's user privilege access criteria*** (Col. 26, Line 61- Col. 28, Line 12).

Regarding to claim 9, Fisher teaches all the claimed subject matters as discussed in claim 7, Fisher further discloses the step of ***establishing an object includes loading information into the object into separate groups having separate access privilege criteria*** (FIG. 15A).

Regarding to claim 10, Fisher teaches all the claimed subject matters as discussed in claim 7, Fisher further discloses the step of ***establishing privilege access criteria includes identifying the separate groups of information to which the user may access*** (FIG. 15A).

Regarding to claim 11, Fisher teaches all the claimed subject matters as discussed in claim 7, Fisher further discloses the step of ***verifying the requestor's user privilege access criteria includes extracting the requestor's user identification from the object request, verifying the requestor's user identification and identifying the groups of data to which the requestor has access*** (Col. 26, Line 61-Col. 28, Line 12).

Regarding to claim 12, Fisher teaches all the claimed subject matters as discussed in claim 7, but does not explicitly teach the step of ***transmitting a redacted object includes sending an electronic object to the requester that contains the groups of information to which the requestor has access to and that excludes groups of information to which the requestor does not have access***. However, as disclosed by Fisher, to limit a user access to the management information stored in the tables, a View can be used to limit access by hiding certain columns and rows from the user (Col. 19, Lines 30-49). As shown in FIG. 11B, a user request for management information includes one or more View names, each View name following the view_tablename_username naming convention. For instance, to read the data in a table named "table 1" for a managed object whose FDN is equal to "/a/b/c," an authorized user named "Max" would use the

SQL command: SELECT*FROM view_table1_max WHERE FDN="a/b/c" (Col. 19, Line 65-Col. 20, Line 7).

User Request
SELECT ... FROM View_name
1102
1104

FIG. 11B

To process the request, the Grant and Deny tables are checked (Col. 26, Line 61-Col. 27, Line 47), and if access is granted, the data read from the DBMS is returned to the requesting user (Col. 27, Line 64-Col. 28, Line 12). As seen, table1 is a table form document, obviously, is rearranged or redacted to have the view_table1_max by blocking out the rows that contain FDN according to the Grant and Deny tables that define a user's privilege for a particular operation, then returning to the requesting user. Thus, the example of view_table1_max, obviously, is ***a redacted document***. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher technique by transmitting a view table as a redacted document to a user in order to represent to a user the managed objects.

Regarding to claim 13, Fisher teaches a system and method for controlling access to managed objects in a computer network.

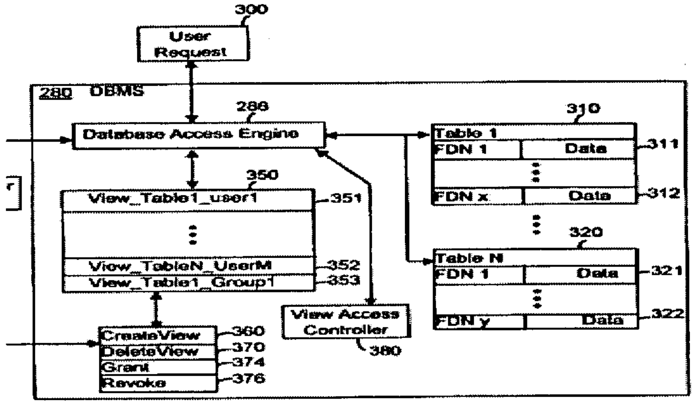
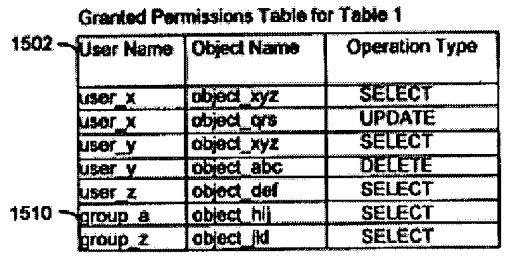


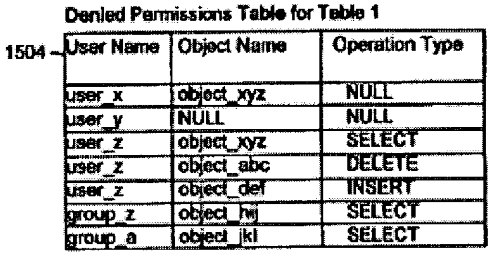
FIG. 10



Granted Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	SELECT
user_x	object_qrs	UPDATE
user_y	object_xyz	SELECT
user_y	object_abc	DELETE
user_z	object_def	SELECT
group_a	object_hij	SELECT
group_z	object_jkl	SELECT

FIG. 15A



Denied Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	NULL
user_y	NULL	NULL
user_z	object_xyz	SELECT
user_z	object_abc	DELETE
user_z	object_def	INSERT
group_z	object_hij	SELECT
group_a	object_jkl	SELECT

FIG. 15B

As shown in FIG. 10 is a conventional DBMS 280 for storing tables 310, 320 (Col. 18, Lines 39-42), wherein each row is the information of a managed object (Col. 19, Lines 4-7). As seen, each row of the tables indicates the technique of ***establishing an object in a storage location***. As shown in FIG. 15A and B (Col. 25, Line 37-Col. 26, Line 52) is the step of ***identifying a user to have access to the object***, and ***establishing privilege access criteria that define the scope of access of the object for the user***. Fisher further discloses the step of ***receiving an object request by a requestor*** (Col. 27, Lines 48-63), and ***verifying the requestor's user privilege access criteria*** (Col. 26, Line 61-Col. 27, Line 47).

Fisher does not explicitly teach the step of ***transmitting a redacted document according to the requestor's user privilege access criteria***. However, as disclosed by Fisher, to limit a user access to the management information stored in the tables, a View can be used to limit access by hiding certain columns and rows from the user (Col. 19, Lines 30-49). As shown in FIG. 11B, a user request for management information includes one or more View names, each View name following the view_tablename_username naming convention. For instance, to read the data in a table named "table 1" for a managed object whose FDN is equal to "/a/b/c," an authorized user named "Max" would use the SQL command: SELECT*FROM view_table1_max WHERE FDN="a/b/c" (Col. 19, Line 65-Col. 20, Line 7).

User Request
SELECT ... FROM View_name
1102
1104

FIG. 11B

To process the request, the Grant and Deny tables are checked (Col. 26, Line 61-Col. 27, Line 47), and if access is granted, the data read from the DBMS is returned to the requesting user (Col. 27, Line 64-Col. 28, Line 12). As seen, table1 is a table form document, obviously, is rearranged or redacted to have the view_table1_max by blocking out the rows that contain FDN according to the Grant and Deny tables that define a user's privilege for a particular operation, then returning to the requesting user. Thus, the example of view_table1_max, obviously, is ***a redacted document***. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher technique by transmitting a view table as a redacted document to a user in order to represent to a user the managed objects.

Regarding to claims 14 and 15, Fisher teaches a system and method for controlling access to managed objects in a computer network.

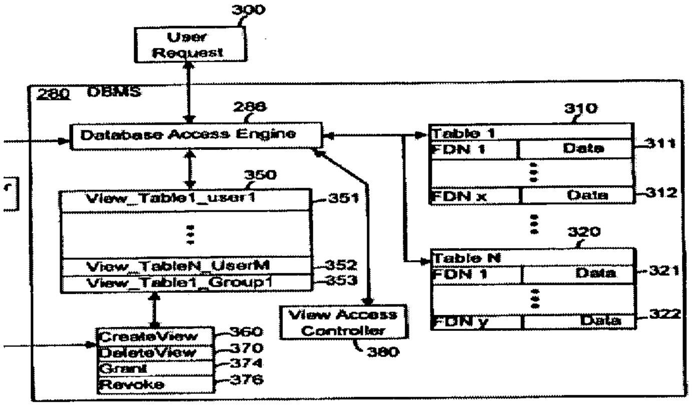
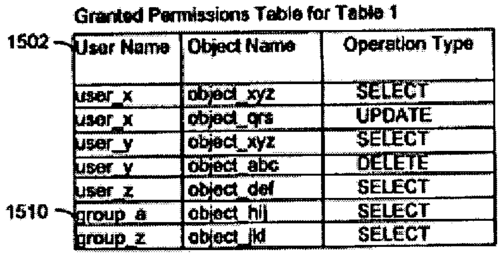


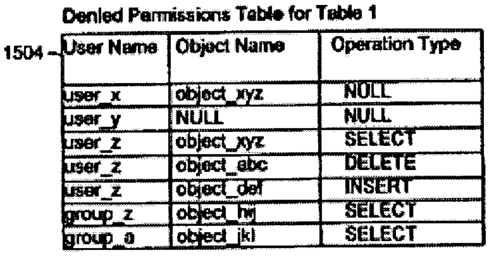
FIG. 10



Granted Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	SELECT
user_x	object_qrs	UPDATE
user_y	object_xyz	SELECT
user_y	object_abc	DELETE
user_z	object_def	SELECT
group_a	object_hij	SELECT
group_z	object_jkl	SELECT

FIG. 15A



Denied Permissions Table for Table 1

User Name	Object Name	Operation Type
user_x	object_xyz	NULL
user_y	NULL	NULL
user_z	object_xyz	SELECT
user_z	object_abc	DELETE
user_z	object_def	INSERT
group_z	object_hij	SELECT
group_a	object_jkl	SELECT

FIG. 15B

As shown in FIG. 10 is a conventional DBMS 280 for storing tables 310, 320 (Col. 18, Lines 39-42), wherein each row is the information of a managed object (Col. 19, Lines 4-7). As seen, each row of the tables indicates the technique of ***establishing an object in a storage location***. As shown in FIG. 15A and B (Col. 25, Line 37-Col. 26, Line 52) is the step of ***identifying a user to have access to the object***, and ***establishing privilege access criteria that define the scope of access of the object for the user***. Fisher further discloses the step of ***receiving an object request by a requestor*** (Col. 27, Lines 48-63), and

verifying the requestor's user privilege access criteria (Col. 26, Line 61-Col. 27, Line 47). Fisher does not explicitly teach the step of ***transmitting a redacted object according to the requestor's user privilege access criteria***. However, as disclosed by Fisher, to limit a user access to the management information stored in the tables, a View can be used to limit access by hiding certain columns and rows from the user (Col. 19, Lines 30-49). As shown in FIG. 11B, a user request for management information includes one or more View names, each View name following the view_tablename_username naming convention. For instance, to read the data in a table named "table 1" for a managed object whose FDN is equal to "/a/b/c," an authorized user named "Max" would use the SQL command: SELECT*FROM view_table1_max WHERE FDN="a/b/c" (Col. 19, Line 65-Col. 20, Line 7).

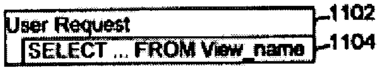


FIG. 11B

To process the request, the Grant and Deny tables are checked (Col. 26, Line 61-Col. 27, Line 47), and if access is granted, the data read from the DBMS is returned to the requesting user (Col. 27, Line 64-Col. 28, Line 12). As seen, table1 is an object as well, obviously, is rearranged or redacted to have the view_table1_max by blocking out the rows that contain FDN according to the Grant and Deny tables that define a user's privilege for a particular operation, then returning to the requesting user. Thus, the example of view_table1_max, obviously, is ***a redacted object***. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher technique by transmitting a view table as a redacted object to a user in order to represent to a user the managed objects.

7. Claims 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher et al. [USP 6,085,191] in view of Applicant Admitted Prior Art [Background].

Regarding to claim 6, Fisher teaches all the claimed subject matters as discussed in claim 1, but does not teach ***the access is determined by a business relationship to produce products and defined by the host according to the need of information in the product chain***. As in the background is the description of a business relationship to produce products and the product chain. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Fisher system by applying the control access technique to a business in order to specify access right to particular users.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to HUNG Q PHAM whose telephone number is 703-605-4242. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JOHN E BREENE can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

9. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner Hung Pham
June 23, 2004

SHAHID ALAM
PRIMARY EXAMINER